LOCC distinguishability of unilaterally transformable quantum states

Somshubhro Bandyopadhyay,* Sibasish Ghosh,† and Guruprasad Kar‡

We consider the question of perfect local distinguishability of mutually orthogonal bipartite quantum states, with the property that every state can be specified by a unitary operator acting on the local Hilbert space of Bob. We show that if the states can be exactly discriminated by one-way LOCC where Alice goes first, then the unitary operators can also be perfectly distinguished by an orthogonal measurement on Bob's Hilbert space. We give examples of sets of $N \leq d$ maximally entangled states in $d \otimes d$ for $d = 4, 5, 6$ that are not perfectly distinguishable by one-way LOCC. Interestingly for $d = 5, 6$ our examples consist of four and five states respectively. We conjecture that these states cannot be perfectly discriminated by two-way LOCC.

PACS number: 03.67.-a, 03.65.Ud, 42.50.-p

I. INTRODUCTION

The question of local discrimination of orthogonal quantum states has received considerable attention in recent years [1–5, 7–15, 18–21]. In the bipartite setting, Alice and Bob share a quantum system prepared in one of a known set of mutually orthogonal quantum states. Their goal is to determine the state in which the quantum system was prepared using only local operations and classical communication (LOCC). In some cases it is possible to identify the state without error while in some others it is not by LOCC alone. For example, while any two orthogonal pure states can be perfectly distinguished by LOCC [3], a complete

*Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Kolkata 700091, India; Electronic address: som@bosemain.boseinst.ac.in

†Optics and Quantum Information Group, The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India ; Electronic address: sibasish@imsc.res.in

‡Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India ; Electronic address: gkar@isical.ac.in

orthogonal basis of entangled states is locally indistinguishable [6, 7, 10]. The nonlocal nature of quantum information is therefore revealed when a set of orthogonal states of a composite quantum system cannot be reliably identified by LOCC. This has been particularly useful to explore quantum nonlocality and its relationship with entanglement [1, 2, 4, 10], and has also found practical applications in quantum cryptography primitives like secret sharing, and data hiding [23–26].

The fundamental result of Walgate et al shows that it is always possible to perfectly discriminate any two orthogonal quantum states by LOCC regardless of their dimension, multipartite structure and entanglement [3]. As it turns out, quite remarkably, perfect discrimination of more than two orthogonal states is not always possible. Examples include, any three orthogonal entangled states in $2 \otimes 2$, two maximally entangled states and a product state in $2 \otimes 2$ and so on [6]. When perfect discrimination is not possible, one may distinguish the states conclusively or unambigously [18–20], where the unknown state is reliably identified with probability less than unity. A necessary and sufficient condition for unambigious discrimination of quantum states, not necessarily orthogonal was obtained by Chefles [20]. Recently, Bandyopadhyay and Walgate has shown that for any set of three states conclusive identification is always possible [16]. In the worst case scenario, only one member of the set, and not all, can be correctly identified, albeit with a non-zero probability.

Interestingly, the maximally entangled basis (Bell basis) in $2 \otimes 2$ [5], or a complete orthogonal entangled basis in $n \otimes m$ [10] are not even conclusively distnguishable, in which case we say that the sets are completely indistinguishable. Note that if an orthogonal set contains at least one product state, one can always distinguish the set conclusively. Therefore, all members of a completely indistinguishable set must necessarily be entangled.

The present work is motivated by the results on local distinguishability of orthogonal maximally entangled states [5, 7, 9, 11], and in particular those that put an upper bound on the number of states that can be perfectly distinguished by LOCC [7, 11]. For example, it was first observed in [7] that no more than d maximally entangled states in $d \otimes d$ can be perfectly distinguished provided the states were chosen from the Bell basis. This was soon followed by a more general result establishing this bound for any set of maximally entangled states in $d \otimes d$ [11].

It is therefore natural to ask whether any N orthogonal maximally entangled states in $d \otimes d$ can be perfectly distinguished by means of a LOCC protocol if $N \leq d$. The general answer is not yet known except in dimensions $2 \otimes 2$ [3] and $3 \otimes 3$ [11]. In $2 \otimes 2$ the answer follows as a corollary of the more general result that any two orthogonal quantum states of a composite quantum system can be reliably distinguished [3]. In [11] a constructive proof was given to show that any three orthogonal maximally entangled states in $3 \otimes 3$ can be perfectly distinguished by LOCC. It is worth noting that in both [3] and [11] the maximally entangled states could be perfectly distinguished by one-way LOCC. Indeed, for almost all known sets of bipartite orthogonal states that are perfectly LOCC distinguishable, one-way protocols are sufficient. A notable exception to this can be found in [1] where it was shown that two-way LOCC is required to distinguish subsets of a locally indistinguishable orthogonal basis of $3 \otimes 3$.

II. FORMULATION OF THE PROBLEM AND RESULTS

In this work we consider the question of perfect LOCC distinguishability of bipartite orthogonal quantum states $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ with the property

$$|\psi_i\rangle = (I \otimes U_i)\,|\psi\rangle, \tag{1}$$

$i = 1, ..., N$ for U_i unitary. Eq. (1) is equivalent to the fact that Bob alone can transform $|\psi_i\rangle$ into $|\psi_j\rangle$ for every pair (i, j). These states are known not to be perfectly distinguishable by LOCC if $N > \dim \mathcal{H}_B$ [11]. Therefore, the only case of interest is $N \leq \dim \mathcal{H}_B$. Clearly, for a given $|\psi_1\rangle$, the states defined by (1) are completely specified by the set of unitary operators $\{U_1, U_2, ..., U_N\}$ on $\mathcal{H}_B$. Let us point out that the maximally entangled states form a subset of the class of sets defined by (1).

The main result of this paper lies in showing that one-way LOCC distinguishability of the states (1) can be completely characterized by distinguishability of the unitary operators $\{U_1, U_2, ..., U_N\}$ acting on Bob's Hilbert space. Before we proceed let us first explain what we mean by distinguishing unitary operators.

A given set of unitary operators $\{U_1, U_2, ..., U_n\}$ acting on some Hilbert space $\mathcal{H}$ is said to perfectly distinguishable in $\mathcal{H}$ if there exists a vector $|\eta\rangle \in \mathcal{H}$ such that

$$\langle \eta | U_i^\dagger U_j | \eta \rangle = \delta_{ij} \tag{2}$$

for all $1 \leq i, j \leq n$. It could so happen that such a vector $|\eta\rangle$ does not exist. This however, does not mean that the unitary operators cannot be reliably distinguished because it may be possible to discriminate them exactly in a locally extended tensor product space.

A set of unitary operators $\{U_1, U_2, ..., U_n\}$ on $\mathcal{H}$ are perfectly distinguishable in an extended tensor product space $\mathcal{H}^{'} \otimes \mathcal{H}$ if there exists a vector $|\zeta\rangle \in \mathcal{H}^{'} \otimes \mathcal{H}$ such that

$$\langle\zeta| \left(I \otimes U_i^{\dagger} U_j\right) |\zeta\rangle = \delta_{ij} \tag{3}$$

for all $1 \leq i, j \leq n$. The above equation simply reflects the orthogonality condition for the vectors $(I \otimes U_i) |\zeta\rangle \in \mathcal{H}^{'} \otimes \mathcal{H}$ for $i = 1, ..., n$. Notice that if (2) holds then so does (3) trivially. The converse however, is not generally true. In this paper we are particularly interested in those unitary operators that cannot be perfectly distinguished in the Hilbert space they act upon but instead they can be distinguished in an extended tensor product space. Notice that as far as distinguishing a set of unitary operators are concerned, the question of LOCC doesn't arise for obvious reasons. The tensor product extension can be done locally by bringing in an ancilla.

We can now state our results.

Proposition 1. *Let $\{U_1, U_2, ..., U_n\}$ be a set of unitary operators on Hilbert space $\mathcal{H}$, where, $n \leq \dim \mathcal{H}$. If the unitary operators can be perfectly distinguished only in an extended tensor product Hilbert space $\mathcal{H}^{'} \otimes \mathcal{H}$, then there exists a set of orthogonal states*

$$|\psi_i\rangle = (I \otimes U_i) |\psi\rangle \tag{4}$$

in $\mathcal{H}^{'} \otimes \mathcal{H}$ for some vector $|\psi\rangle \in \mathcal{H}^{'} \otimes \mathcal{H}$ and $i = 1, ..., n$. The set of states $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle\}$ is not perfectly distinguishable by one-way LOCC in the direction $\mathcal{H}^{'} \rightarrow \mathcal{H}$ where the class of LOCC operations are defined with respect to the tensor product space $\mathcal{H}^{'} \otimes \mathcal{H}$.

An immediate consequence of this result is that if the orthogonal states defined by (1) are perfectly distinguishable by one-way LOCC where Alice goes first, then the local unitary operators $U_1, U_2, ..., U_N$ can also be perfectly distinguished in $\mathcal{H}_B$.

Corollary 1. *Consider a set of mutually orthogonal vectors* $\{|\psi_i\rangle, |\psi_2\rangle, ..., |\psi_N\rangle\}$ *in* $\mathcal{H}_A \otimes \mathcal{H}_B$ *with the property that for every* i, $|\psi_i\rangle = (I \otimes U_i)\,|\psi_1\rangle$ *for* U_i *unitary. Futhermore* $N \leq \dim \mathcal{H}_B$. *If the vectors are perfectly distinguishable by one-way LOCC in the direction* $A \rightarrow B$ *then there exists at least one vector* $|\phi\rangle \in \mathcal{H}_\mathcal{B}$ *such that for all* k, l, *with* $1 \leq k, l \leq N$, $\langle\phi|U_k^\dagger U_l|\phi\rangle = \delta_{kl}$.

Observe that the necessary condition is nontrivial and interesting only if $N \leq \dim \mathcal{H}_B$. Otherwise it is trivially violated. Interestingly if the states are in $2 \otimes d$ then the above condition holds for all two-way LOCC protocols initiated by Alice.

Corollary 2. *Consider a set of mutually orthogonal vectors* $\{|\psi_i\rangle, |\psi_2\rangle, ..., |\psi_N\rangle\} \in \mathcal{H}_A \otimes \mathcal{H}_B$, $\dim \mathcal{H}_A = 2$, $\dim \mathcal{H}_B \geq 2$, *with the property that* $|\psi_i\rangle = (I \otimes U_i)\,|\psi_1\rangle$, $i = 1, ..., N$ *for* U_i *unitary. Furthermore* $N \leq \dim \mathcal{H}_B$. *If the set is perfectly distinguishable by LOCC when Alice goes first, then there exists at least one vector* $|\phi\rangle \in \mathcal{H}_\mathcal{B}$ *such that for any* $k, l \in \{1, 2, ..., N\}$, $\langle\phi|U_k^\dagger U_l|\phi\rangle = \delta_{kl}$.

We apply our results to the case of distinguishing maximally entangled states. We notice that similar property as in (1) holds for maximally entangled states as well. That is, if $|\Psi\rangle$ is a maximally entangled state of $d \otimes d$ then it can be written in terms of the standard maximally entangled state

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle, \tag{5}$$

in the following way:

$$|\Psi\rangle = (I \otimes U)\,|\Phi^+\rangle \tag{6}$$

$$= \left(U^T \otimes I\right)|\Phi^+\rangle \tag{7}$$

where, U is unitary. The following result makes explicit use of the equations (6) and (7) for one-way LOCC in the directions $A \rightarrow B$ and $B \rightarrow A$ respectively.

Corollary 3. *Consider a set of maximally entangled vectors* $\{|\Psi_1\rangle, |\Psi_2\rangle, ..., |\Psi_N\rangle\}$ *in* $\mathcal{H}_A \otimes \mathcal{H}_B$ *where,* $N \leq \dim \mathcal{H}_A = \dim \mathcal{H}_B = d$, *with* $|\Psi_i\rangle = (I \otimes U_i)\,|\Phi^+\rangle$. *If the set is perfectly distinguishable by one-way LOCC in the direction* $A \rightarrow B$, *then there exists at least one vector* $|\phi\rangle \in \mathcal{H}_B$ *such that,* $\langle\phi|U_k^\dagger U_l|\phi\rangle = \delta_{kl}$

for $1 \leq k, l \leq N$*. On the other hand if the set is perfectly distinguishable by one-way LOCC in the direction* $B \rightarrow A$*, then there exists at least one vector* $|\phi^{'}\rangle \in \mathcal{H}_A$ *so that* $\langle\phi^{'}|V_k^{\dagger}V_l|\phi^{'}\rangle = \delta_{kl}$ *for* $1 \leq k, l \leq N$*, where* $V_k = U_k^T$*.*

We note that the known cases in which a set of maximally entangled states can be perfectly distinguished by LOCC (these LOCC protocols are all one-way in the direction $A \rightarrow B$ [7, 9, 11]), the orthogonal measurements on Bob's Hilbert space make explicit use of vectors $\{|\phi_m\rangle\} \in \mathcal{H}_B$ with the property $\langle\phi_m|U_k^{\dagger}U_l|\phi_m\rangle = \delta_{kl}$ for every m and for all k and l.

Given the existing symmetry in maximally entangled states one might wonder whether there is any difference between the one-way LOCC protocols "Alice goes first" and "Bob goes first". This is an interesting question and intuitively it seems that for distinguishing maximally entangled states this should not be an issue. However we haven't been able to conclusively prove that this is the case. As noted in Corollary 3, if the states are perfectly distinguishable when Bob goes first then the orthogonality condition

$$\langle\phi^{'}|V_k^{\dagger}V_l|\phi^{'}\rangle = \delta_{kl} \tag{8}$$

must hold for all k and l for some $|\phi^{'}\rangle$. Using the fact that $V_k = U_k^T$ the above equation can also be written as

$$\langle\phi^{'}|U_k^{*}U_l^{T}|\phi^{'}\rangle = \delta_{kl} \tag{9}$$

which in turn is equivalent to the condition

$$\langle\phi^{*'}|U_l U_k^{\dagger}|\phi^{*'}\rangle = \delta_{kl}. \tag{10}$$

Comparing the above condition with that of one-way LOCC in the direction $A \rightarrow B$ (as mentioned in Corollary 1) it is not clear if there is any one-to-one correspondence between the two. So we conclude that if the maximally entangled states are perfectly distinguishable by one-way LOCC in the direction $A \rightarrow B$, then they can also be perfectly distinguished in the opposite direction provided $\left[U_k^{\dagger}, U_l\right] = 0$ for all $k, l = 1, ..., N$. In the latter case one can of course choose $|\phi^{'}\rangle = |\phi^{*}\rangle$.

III. ONE-WAY LOCC INDISTINGUISHABLE MAXIMALLY ENTANGLED STATES

We now give examples of one-way locally indistinguishable sets of N orthogonal maximally entangled states in $d \otimes d$, where $N \leq d$ and $d = 4, 5, 6$. Our examples constitute the following: (a) a set of four maximally entangled states in $4 \otimes 4$, (b) a set of four maximally entangled states in $5 \otimes 5$, and (c) a set five maximally entangled states in $6 \otimes 6$. To show that these states are locally indistinguishable by all one-way LOCC protocols it suffices to show (see Corollary 3) that the local unitary operators (or their transposes) cannot be perfectly distinguished in $\mathcal{H}_B$ (or $\mathcal{H}_A$). We provide complete proofs for all the examples.

The maximally entangled states considered in these examples belong to the family of generalized Bell states. In $d \otimes d$, d^2 generalized Bell states written in the standard basis can be expressed as,

$$|\Psi_{nm}^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{\frac{2\pi i j n}{d}} |j\rangle \otimes |j \oplus_d m\rangle \tag{11}$$

for $n, m = 0, 1, \cdots, d-1$, where, $j \oplus_d m \equiv (j+m) \mod d$. The standard maximally entangled state $|\Phi^+\rangle$ in $d \otimes d$ is simply $|\Psi_{00}^{(d)}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$. These states are related to the standard maximally entangled state in the following way,

$$\left(I \otimes U_{nm}^{(d)}\right) |\Psi_{00}\rangle = |\Psi_{nm}^{(d)}\rangle \tag{12}$$

where,

$$U_{nm}^{(d)} = \sum_{j=0}^{d-1} e^{\frac{2\pi i j n}{d}} |j \oplus_d m\rangle\langle j| \tag{13}$$

are $d \times d$ unitary matrices for $n, m = 0, 1, \cdots, d-1$.

Example 1. *The following four maximally entangled states* $|\Psi_{00}^{(4)}\rangle, |\Psi_{11}^{(4)}\rangle, |\Psi_{32}^{(4)}\rangle, |\Psi_{31}^{(4)}\rangle$ *in* $4 \otimes 4$ *are not perfectly distinguishable by one-way LOCC.*

Example 2. *The following four maximally entangled states* $|\Psi_{00}^{(5)}\rangle, |\Psi_{01}^{(5)}\rangle, |\Psi_{31}^{(5)}\rangle, |\Psi_{22}^{(5)}\rangle$ *in* $5 \otimes 5$ *are not perfectly distinguishable by one-way LOCC.*

Example 3. *The following five maximally entangled states* $|\Psi_{00}^{(6)}\rangle, |\Psi_{01}^{(6)}\rangle, |\Psi_{41}^{(6)}\rangle, |\Psi_{12}^{(6)}\rangle, |\Psi_{33}^{(6)}\rangle$ *in* $6 \otimes 6$ *are not perfectly distinguishable by one-way LOCC.*

IV. PROOFS

Proof of Proposition 1: Assume that the unitary operators $U_1, U_2, ..., U_n$ acting on $\mathcal{H}$ can only be distinguished in an extended tensor product space $\mathcal{H}' \otimes \mathcal{H}$. This implies that there does not exist any vector $|\phi\rangle \in \mathcal{H}$, such that for all k, l, with $1 \leq k, l \leq n$,

$$\langle\phi|U_k^\dagger U_l|\phi\rangle = \delta_{kl}. \tag{14}$$

We will now show that if the set of states $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle\}$ defined by Eq. (4) is perfectly distinguishable by one-way LOCC in the direction $\mathcal{H}^{'} \to \mathcal{H}$ where the class of LOCC operations are defined with respect to the tensor product space $\mathcal{H}^{'} \otimes \mathcal{H}$, then there must exist a vector $|\phi\rangle \in \mathcal{H}$, such that for all k, l, with $1 \leq k, l \leq n$,

$$\langle\phi|U_k^\dagger U_l|\phi\rangle = \delta_{kl}. \tag{15}$$

Suppose that the states $|\psi_1\rangle, ..., |\psi_n\rangle \in \mathcal{H}' \otimes \mathcal{H}$ are perfectly distinguishable by one-way LOCC in the direction $\mathcal{H}^{'} \to \mathcal{H}$. Let $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2, \cdots, \}$ be the POVM of the local measurement on $\mathcal{H}'$ satisfying the usual constraints that $\{\mathcal{A}_i\}$ are positive operators and $\sum_i A_i \leq \mathcal{I}_{\mathcal{H}'}$. Associated with the i^{th} outcome, let $\mathcal{B}^i = \{\mathcal{B}_{ij}\}$ be the POVM of the local measurement on $\mathcal{H}$ satisfying $\sum_j \mathcal{B}_{ij} \leq \mathcal{I}_{\mathcal{H}}$ where $\{\mathcal{B}_{ij}\}$ are positive operators. It may be noted that by defining $\mathcal{B}_i = \sum_j \mathcal{B}_{ij}$, the collection of positive operators $\{\mathcal{A}_i \otimes \mathcal{B}_i\}$ represents a separable POVM satisfying $\sum_i \mathcal{A}_i \otimes \mathcal{B}_i \leq I_{\mathcal{H}' \otimes \mathcal{H}}$.

Let $\mathcal{A}_i = A_i^\dagger A_i$, where A_i is the Kraus element. Subsequent to the i^{th} outcome of the measurement $\mathcal{A}$, the reduced density matrix on $\mathcal{H}$ (for the input state $|\psi_k\rangle$) is given by

$$\sigma_{k,A_i} = \mathrm{Tr}_A \frac{\rho_k \mathcal{A}_i \otimes I}{\mathrm{Tr}\left(\rho_k \mathcal{A}_i \otimes I\right)}, \tag{16}$$

where, $\rho_k = |\psi_k\rangle\langle\psi_k|$. Because a measurement now perfectly distinguishes the set of reduced density matrices $\{\sigma_{k,A_i} \in \mathcal{H} : k = 1, ..., n\}$, they must be mutually orthogonal, that is,

$$\mathrm{Tr}\left(\sigma_{k,A_i}\sigma_{l,A_i}\right) = 0 \, : k \neq l \tag{17}$$

Noting that the states we are trying to perfectly distinguish are of the form,

$$|\psi_k\rangle = \left(I \otimes U_k\right)|\psi_1\rangle \tag{18}$$

for $k = 1, ..., n$; the transformed state $|\psi_{k,A_i}\rangle$ (unnormalized) post measurement on $\mathcal{H}'$ is given by

$$|\psi_{k,A_i}\rangle = (A_i \otimes I)(I \otimes U_k)|\psi_1\rangle = (I \otimes U_k)|\psi_{1,A_i}\rangle \tag{19}$$

This in turn implies that the reduced density matrices σ_{k,A_i} for all k, can be expressed in terms of σ_{1,A_i} as,

$$\sigma_{k,A_i} = U_k \sigma_{1,A_i} U_k^\dagger \tag{20}$$

Let the spectral decomposition of the density matrix $\sigma_{1.A_i}$ be,

$$\sum_{p=1}^{r} \lambda_p^i |\chi_p^i\rangle\langle\chi_p^i| \tag{21}$$

where, $0 < \lambda_p^i \leq 1$, $\sum_{p=1}^{r} \lambda_p^i = 1$, and $\langle\chi_p^i|\chi_q^i\rangle = \delta_{pq}$. Using the Eqs. (20) and (21) we can rewrite σ_{k,A_i} as,

$$\sigma_{k,A_i} = \sum_{p=1}^{r} \lambda_p^i U_k |\chi_p^i\rangle\langle\chi_p^i| U_k^\dagger \tag{22}$$

We now apply the orthogonality condition:- $\mathrm{Tr}\left(\sigma_{k,A_i}\sigma_{l,A_i}\right) = 0$, if $k \neq l$ to obtain,

$$\mathrm{Tr}\left(\sigma_{k,A_i}\sigma_{l,A_i}\right) = \sum_{p} \left(\lambda_p^i\right)^2 |\langle\chi_p^i|U_k^\dagger U_l|\chi_p^i\rangle|^2 + \sum_{p \neq q} \lambda_p^i \lambda_q^i |\langle\chi_p^i|U_k^\dagger U_l|\chi_q^i\rangle|^2 = 0 \tag{23}$$

from which it follows that every term in the summation must be identically zero. This is because each term is non-negative (note that $0 < \lambda_p^i \leq 1$) and by adding all the terms we get zero. Moreover, Eq. (23) holds for all k and l. Therefore for every p we have,

$$|\langle\chi_p^i|U_k^\dagger U_l|\chi_p^i\rangle|^2 = 0 \tag{24}$$

from which it follows that there exist vectors $\{|\chi_p\rangle, U_k|\chi_p\rangle \in \mathcal{H} : k = 2, ..., n\}$ forming an orthogonal set. This is in contradiction with the fact that the unitary operators are distinguishable only in an extended tensor product space. This proves the result. $\square$

Remark 1: As noted before Corollary 1 is a direct consequence of Proposition 1. The result of Corollary 2, however, holds for all two way LOCC protocols initiated by Alice. The proof is given below.

Proof of Corollary 2: We assume that the set of vectors $\{|\psi_i\rangle : i = 1, ..., N\} \in 2 \otimes d$ can be perfectly distinguished by LOCC if Alice goes first. From a result in [4] it follows that there exists a basis $\{|0\rangle, |1\rangle\}$ for Alice such that in that basis,

$$|\psi_i\rangle = |0\rangle|\chi_i^0\rangle + |1\rangle|\chi_i^1\rangle \tag{25}$$

where, $\langle\chi_i^0|\chi_j^0\rangle = \langle\chi_i^1|\chi_j^1\rangle = 0$ if $i \neq j$. Using the fact that for every i,

$$|\psi_i\rangle = (I \otimes U_i)\,|\psi_1\rangle, \tag{26}$$

where, U_i is unitary, (25) can be rewritten as

$$|\psi_i\rangle = |0\rangle U_i|\chi_1^0\rangle + |1\rangle U_i|\chi_1^1\rangle \tag{27}$$

where the states $\{U_i|\chi_1^x\rangle\ : x = 0, 1\ : i = 1, ..., N\}$ satisfy the following orthogonality conditions

$$\langle\chi_1^0|U_i^\dagger U_j|\chi_1^0\rangle = \langle\chi_1^1|U_i^\dagger U_j|\chi_1^1\rangle = 0 \tag{28}$$

if $i \neq j$. This concludes the proof. □

Proof of Corollary 3: We first note that a given set of orthogonal maximally entangled vectors can be written in the form of Eq. (4) by virtue of Eq. (6). Clearly the results of Proposition 1 and Corollary 1 apply for one way LOCC protocols in the direction $A \to B$ where the corresponding unitary operators acting on Bob's Hilbert space are denoted by $U_1, ..., U_N$. On the other hand owing to Eq. (7) we know that the same given set of maximally entangled states can also be defined by the action of unitary operators $U_1^T, ..., U_N^T$ acting only on the local Hilbert space of Alice. Thus the results of Proposition 1 and Corollary 1 also apply to one-way LOCC protocols in the direction $B \to A$. □

V. PROOFS OF THE EXAMPLES

Proof of Example 1. We will show that the states are not perfectly distinguishable by one-way LOCC in the direction $A \to B$. A similar proof can be worked out in the direction $B \to A$. We write the states

as: $|\Psi_{00}^{(4)}\rangle, |\Psi_{11}^{(4)}\rangle = \left(I\otimes U_{11}^{(4)}\right)|\Psi_{00}^{(4)}\rangle, |\Psi_{32}^{(4)}\rangle = \left(I\otimes U_{32}^{(4)}\right)|\Psi_{00}^{(4)}\rangle$, and $|\Psi_{31}^{(4)}\rangle = \left(I\otimes U_{31}^{(4)}\right)|\Psi_{00}^{(4)}\rangle$. From Corollary 3, a necessary condition for these four states to be perfectly distinguishable by one-way LOCC in the direction $A\to B$ is that there must exist a vector (normalized) $|\phi\rangle = \sum_{j=0}^{3}\phi_j|j\rangle \in \mathcal{H}_B$ satisfying the normalization condition

$$\sum_{j-0}^{3}|\phi_j|^2 = 1 \tag{29}$$

such that the following four vectors $|\phi\rangle, U_{11}^{(4)}|\phi\rangle, U_{32}^{(4)}|\phi\rangle, U_{31}^{(4)}|\phi\rangle$ are pairwise orthogonal. From here on we will omit the superscript in the unitaries. It is easy to verify that the six unitary operators $U_{11}, U_{31}, U_{32}, U_{11}^{\dagger}U_{32}, U_{11}^{\dagger}U_{31}, U_{32}^{\dagger}U_{31}$ are all distinct. We now write the orthogonality conditions:

$$\langle\phi|U_{11}|\phi\rangle = \sum_{j-0}^{3}\omega^{j}\phi_j\phi^*_{j\oplus_4 1} \;=\; 0, \tag{30}$$

$$\langle\phi|U_{31}|\phi\rangle = \sum_{j=0}^{3}\omega^{3j}\phi_j\phi^*_{j\oplus_4 1} \;=\; 0, \tag{31}$$

$$\langle\phi|U_{32}|\phi\rangle = \sum_{j=0}^{3}\omega^{3j}\phi_j\phi^*_{j\oplus_4 2} \;=\; 0, \tag{32}$$

$$\langle\phi|U_{11}^{\dagger}U_{32}|\phi\rangle = \sum_{j=0}^{3}\omega^{2j}\phi_j\phi^*_{j\oplus_4 1} \;=\; 0, \tag{33}$$

$$\langle\phi|U_{11}^{\dagger}U_{31}|\phi\rangle = \sum_{j=0}^{3}\omega^{2j}|\phi_j|^2 \;=\; 0, \tag{34}$$

$$\langle\phi|U_{32}^{\dagger}U_{31}|\phi\rangle = \sum_{j=0}^{3}\phi_j\phi^*_{j\oplus_4 3} \;=\; 0, \tag{35}$$

where all the exponents of $\omega = e^{\frac{2\pi i}{4}}$ are taken to be numbers addition modulo 4. From Eqs. (30), (31)and (33) one finds that the the vector $(\phi_0^*\phi_1, \phi_1^*\phi_2, \phi_2^*\phi_3, \phi_3^*\phi_0) \in \mathbb{C}^4$ is orthogonal to the following three vectors: $\left(1,\omega,\omega^2,\omega^3\right)$, $\left(1,\omega^3,\omega^2,\omega\right)$, and $\left(1,\omega^2,1,\omega^2\right)$. Therefore, we must have,

$$(\phi_0^*\phi_1, \phi_1^*\phi_2, \phi_2^*\phi_3, \phi_3^*\phi_0) = \lambda\,(1,1,1,1) \tag{36}$$

for some $\lambda\in\mathbb{C}$. We will show that the above equality cannot be satisfied except when $\phi_i = 0$ for every i and $\lambda = 0$ thereby completing the proof. To show this we need to consider two cases, namely, $\lambda\neq 0$ and

$\lambda = 0$.

Case 1 ($\lambda \neq 0$): From Eq. (36)), here we must have, $\forall j,\ \phi_j \neq 0$. Thus for $j = 0, 1, 2, 3$, we have the following two relations:

$$\phi_j^* \phi_{j\oplus_4 2} = \frac{\lambda^2}{|\phi_{j\oplus_4 1}|^2},$$
$$\phi_j^* \phi_{j\oplus_4 3} = \frac{\lambda^3}{|\phi_{j\oplus_4 1}\phi_{j\oplus_4 2}|^2}.$$

Then from Eq. (35) we see that

$$\lambda^{*3} \sum_{j=0}^{3} \frac{1}{|\phi_{j\oplus_4 1}\phi_{j\oplus_4 2}|^2} = 0$$

immediately implying that $\lambda = 0$ which is a contradiction.

Case 2 ($\lambda = 0$): Here the nontrivial cases arise only when any two ϕ_is are zero and the remaining two are non-zero. It is simple to verify that a contradiction is always reached. For example, suppose $\phi_0 = \phi_2 = 0$ and $\phi_1 \neq 0$, $\phi_3 \neq 0$. From Eq. (34) we obtain $|\phi_1|^2 + |\phi_3|^2 = 0$, which immediately implies that $\phi_1 = \phi_3 = 0$. This therefore completes the proof. $\square$

Proof of example 2: We will prove local indistinguishability in the direction $A \to B$. A similar proof holds for $B \to A$ as well. Consider the following four maximally entangled states in $5 \otimes 5$:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{5}} \sum_{j=0}^{4} |jj\rangle$$

$$|\Psi_{n_1 1}\rangle = (I \otimes U_{n_1 1})\, |\Psi_{00}\rangle,$$

$$|\Psi_{n_1' 1}\rangle = \left(I \otimes U_{n_1' 1}\right) |\Psi_{00}\rangle,$$

$$|\Psi_{n_2 2}\rangle = (I \otimes U_{n_2 2})\, |\Psi_{00}\rangle.$$

According to Corollary 3, a necessary condition for these four states to be perfectly distinguishable by one-way LOCC in the direction $A \to B$, is that there must exist a vector (normalized) $|\phi\rangle = \sum_{j=0}^{4} \phi_j |j\rangle \in \mathcal{H}_B$ satisfying the normalization condition

$$\sum_{j-0}^{4} |\phi_j|^2 = 1 \tag{37}$$

and such that the following four vectors $|\phi\rangle, U_{n_1 1}|\phi\rangle, U_{n_1' 1}|\phi\rangle, U_{n_2 2}|\phi\rangle$ are pairwise orthogonal. We now write the orthogonality conditions:

$$\langle\phi|U_{n_1 1}|\phi\rangle = \sum_{j=0}^{4} \omega^{n_1 j}\phi_j\phi^*_{j\oplus_5 1} \;=\; 0, \tag{38}$$

$$\langle\phi|U_{n_1' 1}|\phi\rangle = \sum_{j=0}^{4} \omega^{n_1' j}\phi_j\phi^*_{j\oplus_5 1} \;=\; 0, \tag{39}$$

$$\langle\phi|U^\dagger_{n_1 1}U_{n_2 2}|\phi\rangle = \sum_{j=0}^{4} \omega^{(n_2-n_1)j}\phi_j\phi^*_{j\oplus_5 1} \;=\; 0, \tag{40}$$

$$\langle\phi|U^\dagger_{n_1' 1}U_{n_2 2}|\phi\rangle = \sum_{j=0}^{4} \omega^{(n_2-n_1')j}\phi_j\phi^*_{j\oplus_5 1} \;=\; 0, \tag{41}$$

$$\langle\phi|U_{n_2 2}|\phi\rangle = \sum_{j=0}^{4} \omega^{n_2 j}\phi_j\phi^*_{j\oplus_5 2} \;=\; 0, \tag{42}$$

$$\langle\phi|U^\dagger_{n_1 1}U_{n_1' 1}|\phi\rangle = \sum_{j=0}^{3} \omega^{(n_1'-n_1)j}|\phi_j|^2 \;=\; 0, \tag{43}$$

where all the exponents of $\omega = e^{\frac{2\pi i}{5}}$ are taken to be numbers addition modulo 5. For the set of values $n_1 = 0, n_1' = 3$, and $n_2 = 2$ (other suitable choices of n_1, n_1', n_2 are also possible) from Eqs. (38)-(41 we see that the vector $(\phi_0^*\phi_1, \phi_1^*\phi_2, \phi_2^*\phi_3, \phi_3^*\phi_4, \phi_4^*\phi_5) \in \mathbb{C}^5$ is orthogonal to the set of following four vectors $\left\{(1,1,1,1,1), \left(1,\omega^3,\omega,\omega^4,\omega^2\right), \left(1,\omega^2,\omega^4,\omega,\omega^3\right), \left(1,\omega^4,\omega^3,\omega^2,\omega\right)\right\} \in \mathbb{C}^5$. Noting that the vector $\left(1,\omega,\omega^2,\omega^3,\omega^4\right)$ is orthogonal to the previous four vectors, the following identity

$$(\phi_0^*\phi_1, \phi_1^*\phi_2, \phi_2^*\phi_3, \phi_3^*\phi_4, \phi_4^*\phi_5) = \lambda\left(1,\omega,\omega^2,\omega^3,\omega^4\right) \tag{44}$$

must be valid for some $\lambda \in \mathbb{C}^5$. Proceeding as in example 1, we need to consider two cases, namely, $\lambda \neq 0$ and $\lambda = 0$.

Case 1 ($\lambda \neq 0$): This means that $\phi_j \neq 0$ for all $j = 01, 2, 3, 4$. Using Eq. (44) in Eq. (42) we see that

$$\lambda^{*^2}\omega^4 \sum_{j=0}^{4} \frac{1}{|\phi_{j\oplus_5 1}|^2} = 0,$$

implying that $\lambda = 0$, which is a contradiction.

Case 2 ($\lambda = 0$): Here we need to consider several possibilities depending upon the values of ϕ_is. A straightforward but tedious calculation shows that all the possibilties are ruled out for not being able to satisfy the orthogonality conditions and Eq. (44) simultaneously unless $|\phi\rangle$ is a null vector. This therefore completes the proof. □

Proof of example 3. As in the proof of the previous example, we begin with a more general family of five orthogonal states in $6 \otimes 6$. We will prove the local indistinguishability in the direction $A \to B$. We note that a similar proof holds in the direction $B \to A$ as well. The states are defined as follows:

$$\begin{aligned}
|\Psi_{00}\rangle &= \frac{1}{\sqrt{6}} \sum_{j=0}^{5} |jj\rangle, \\
|\Psi_{n_1 1}\rangle &= (I \otimes U_{n_1 1})\, |\Psi_{00}\rangle, \\
|\Psi_{n_1' 1}\rangle &= \left(I \otimes U_{n_1' 1}\right) |\Psi_{00}\rangle, \\
|\Psi_{n_2 2}\rangle &= (I \otimes U_{n_2 2})\, |\Psi_{00}\rangle, \\
|\Psi_{n_3 3}\rangle &= (I \otimes U_{n_3 3})\, |\Psi_{00}\rangle,
\end{aligned}$$

where, $U_{nm} = \sum_{j=0}^{5} e^{\frac{2n\pi ij}{6}} |j \oplus_6 m\rangle\langle n|$, with $n, m = 0, 1, 2, 3, 4, 5$ and $j \oplus_6 m = (j + m) \,\mathrm{mod} 6$. Also, we denote $\omega = e^{\frac{2\pi i}{6}}$.

From Corollary 3, a necessary condition that the above five states to be perfectly distinguishable by one way LOCC in the direction $A \to B$ is that there must exist a normalized vector $|\phi\rangle = \sum_{j=0}^{5} \phi_j |j\rangle \in \mathbb{C}^6$ satisfying the normalization condition

$$\sum_{j=0}^{5} |\phi_j|^2 = 1 \tag{45}$$

and such that the following five vectors $|\phi\rangle, U_{n_1 1}|\phi\rangle, U_{n_1' 1}|\phi\rangle, U_{n_2 2}|\phi\rangle$ and $U_{n_3 3}|\phi\rangle$ are pairwise orthogonal.

The orthogonality conditions can be written as,

$$\langle\phi|U_{n_1 1}|\phi\rangle = \sum_{j=0}^{5}\omega^{n_1 j}\phi_j\phi^*_{j\oplus_6 1} = 0, \tag{46}$$

$$\langle\phi|U_{n'_1 1}|\phi\rangle = \sum_{j=0}^{5}\omega^{n'_1 j}\phi_j\phi^*_{j\oplus_6 1} = 0, \tag{47}$$

$$\langle\phi|U^\dagger_{n_1 1}U_{n_2 2}|\phi\rangle = \sum_{j=0}^{5}\omega^{(n_2-n_1)j}\phi_j\phi^*_{j\oplus_6 1} = 0, \tag{48}$$

$$\langle\phi|U^\dagger_{n'_1 1}U_{n_2 2}|\phi\rangle = \sum_{j=0}^{5}\omega^{\left(n_2-n'_1\right)j}\phi_j\phi^*_{j\oplus_6 1} = 0, \tag{49}$$

$$\langle\phi|U^\dagger_{n_2 2}U_{n_3 3}|\phi\rangle = \sum_{j=0}^{5}\omega^{(n_3-n_2)j}\phi_j\phi^*_{j\oplus_6 1} = 0, \tag{50}$$

$$\langle\phi|U_{n_2 2}|\phi\rangle = \sum_{j=0}^{5}\omega^{n_2 j}\phi_j\phi^*_{j\oplus_6 2} = 0, \tag{51}$$

$$\langle\phi|U^\dagger_{n_1 1}U_{n_3 3}|\phi\rangle = \sum_{j=0}^{5}\omega^{(n_3-n_1)j}\phi_j\phi^*_{j\oplus_6 2} = 0, \tag{52}$$

$$\langle\phi|U^\dagger_{n'_1 1}U_{n_3 3}|\phi\rangle = \sum_{j=0}^{5}\omega^{\left(n_3-n'_1\right)j}\phi_j\phi^*_{j\oplus_6 2} = 0, \tag{53}$$

$$\langle\phi|U_{n_3 3}|\phi\rangle = \sum_{j=0}^{5}\omega^{n_3 j}\phi_j\phi^*_{j\oplus_6 3} = 0, \tag{54}$$

$$\langle\phi|U^\dagger_{n_1 1}U_{n'_1 1}|\phi\rangle = \sum_{j=0}^{5}\omega^{\left(n'_1-n_1\right)j}|\phi_j|^2 = 0, \tag{55}$$

We choose here $n_1 = 0$, $n'_1 = 4$, $n_2 = 1$, and $n_3 = 3$. Let us note that the proof holds for other suitable choices as well. From Eqs. (46) to (50) we see that the vector $(\phi^*_0\phi_1, \phi^*_1\phi_2, \phi^*_2\phi_3, \phi^*_3\phi_4, \phi^*_4\phi_5, \phi^*_5\phi_0) \in \mathbb{C}^6$ is orthogonal to the incomplete basis $\mathcal{B} \in \mathbb{C}^6$ consisting of the following five vectors:
$\left(1, \omega^{n_1}, \omega^{2n_1}, \omega^{3n_1}, \omega^{4n_1}, \omega^{5n_1}\right)$, $\left(1, \omega^{n'_1}, \omega^{2n'_1}, \omega^{3n'_1}, \omega^{4n'_1}, \omega^{5n'_1}\right)$, $\left(1, \omega^{(n_2-n_1)}, \omega^{2(n_2-n_1)}, \omega^{3(n_2-n_1)}, \omega^{4(n_2-n_1)}, \omega^{5(n_2-n_1)}\right)$, $\left(1, \omega^{\left(n_2-n'_1\right)}, \omega^{2\left(n_2-n'_1\right)}, \omega^{3\left(n_2-n'_1\right)}, \omega^{4\left(n_2-n'_1\right)}, \omega^{5\left(n_2-n'_1\right)}\right)$, $\left(1, \omega^{(n_3-n_2)}, \omega^{2(n_3-n_2)}, \omega^{3(n_3-n_2)}, \omega^{4(n_3-n_2)}, \omega^{5(n_3-n_2)}\right)$.

Note that the vector $\left(1, \omega^{n_4}, \omega^{2n_4}, \omega^{3n_4}, \omega^{4n_4}, \omega^{5n_4}\right)$, with $n_4 = 5$, completes the above mentioned basis.

Therefore we must have the following relation

$$\left(\phi_0^*\phi_1, \phi_1^*\phi_2, \phi_2^*\phi_3, \phi_3^*\phi_4, \phi_4^*\phi_5, \phi_5^*\phi_0\right) = \lambda\left(1, \omega^{n_4}, \omega^{2n_4}, \omega^{3n_4}, \omega^{4n_4}, \omega^{5n_4}\right) \tag{56}$$

to hold true for some $\lambda \in \mathbb{C}$, and $n_4 = 5$. Now from Eqs. (46) to (50) we also obtain that

$$\phi_j^*\phi_{j\oplus 1} = \lambda\omega^{n_4 j}\ \forall j = 0, 1, 2, 3, 4, 5 \tag{57}$$

We now have to consider two cases, namely when $\lambda \neq 0$ and $\lambda = 0$.

Case 1: Let $\lambda \neq 0$. Using Eq. (57) into Eq. (54) we see that

$$\lambda^{*^3}\omega^{3n_4}\sum_{j=0}^{5}\frac{\omega^{(n_3+3n_4)j}}{|\phi_{j\oplus 1}\phi_{j\oplus 2}|^2} = 0 \tag{58}$$

from which we readily obtain $\lambda = 0$ (note that $n_3 + 3n_4 = 0\,\mathrm{mod}6$) which is a contradiction.

Case 2: Let $\lambda = 0$. This gives rise to several subcases that need to be considered individually.

Case 2.1: In this case we assume any five elements of the set $\{\phi_i : i = 0, ..., 5\}$ are zero. Suppose $\phi_5 \neq 0$, and the rest are all zero. The normalization condition implies that $|\phi_5|^2 = 1$. On the other hand from Eq. (55) we see that $\omega^{5\left(n_1'-n_1\right)}|\phi_5|^2 = 0$, thus arriving at a contradiction. Similarly contradictions can be reached for ther cases as well.

Case 2.2: Here we assume any four elements of the set $\{\phi_i : i = 0, ..., 5\}$ are zero. Suppose $\phi_0 = \phi_1 = \phi_2 = \phi_3 = 0$. This clearly violates Eq. (57) and hence this is not possible. Likewise other cases can also be ruled out. Nevertheless it is instructive to look at another case in which the proof is slightly more nontrivial. Suppose $\phi_0 = \phi_1 = \phi_2 = \phi_4 = 0$. Here from Eqs. (51), (52), and (53) we obtain

$$\phi_3\phi_5^* = 0, \tag{59}$$

and from Eq. (55)

$$|\phi_3|^2 + \omega^{2\left(n_1'-n_1\right)}|\phi_5|^2 = 0, \tag{60}$$

and from the normalization condition we get,

$$|\phi_3|^2 + |\phi_5|^2 = 1. \tag{61}$$

Clearly the above three equations are incompatible.

Case 2.3: Here we assume any three elements of the set $\{\phi_i : i = 0, ..., 5\}$ are zero. One can show that all the cases can be ruled out because contradictions are reached with the orthogonality conditions and/or Eq. (57). We give two instances for better understanding of the readers. If we take $\phi_0 = \phi_1 = \phi_2 = 0$, then this is clearly in contradiction with Eq. (57). Somewhat more complicated is the proof of the case corresponding to $\phi_0 = \phi_2 = \phi_4 = 0$. From Eqs. (51), (52), and (53), and explicitly substituting the values $n_1 = 0$, $n_1' = 4$, $n_2 = 1$, and $n_3 = 3$, one can show after some simple algebra that the vector $(\phi_1^*\phi_3, \phi_3^*\phi_5, \phi_5^*\phi_1) \in \mathbb{C}^3$ is a null vector. That is,

$$(\phi_1^*\phi_3, \phi_3^*\phi_5, \phi_5^*\phi_1) = (0, 0, 0) \tag{62}$$

On the other hand Eqs. (55) and the normalization condition give us the following two relations:

$$|\phi_1|^2 + \omega^{2(n_1'-n_1)}|\phi_3|^2 + \omega^{4(n_1'-n_1)}|\phi_5|^2 \;=\; 0 \tag{63}$$

$$|\phi_1|^2 + |\phi_3|^2 + |\phi_5|^2 \;=\; 1 \tag{64}$$

The above three equations are clearly inconsistent with each other.

The remaining cases, namely when any two of the elements are zero and only one element is zero, are easily shown to be ruled out for they all give rise to conradiction with Eq. (57). This completes the proof. Thus we have shown that the five maximally entangled states $|\Psi_{00}^{(6)}\rangle, |\Psi_{01}^{(6)}\rangle, |\Psi_{41}^{(6)}\rangle, |\Psi_{12}^{(6)}\rangle, |\Psi_{33}^{(6)}\rangle$ in $6 \otimes 6$ are not perfectly distinguishable by one way LOCC. $\square$

VI. DISCUSSIONS AND CONCLUSIONS

We have considered in this work one way local distinguishability of a set of orthogonal states which are unilaterally transformable. That is to say, the states can be mapped onto one another by unitary operators acting on the local Hilbert spaces. We have shown that the one-way local distinguishability of such states is initimately related to the question of perfect distinguishability of the corresponding unitary operators in the local Hilbert space they act upon. In particular, if the unitary operators cannot be distinguished in their local Hilbert space but instead are perfectly distinguishable in an extended Hilbert space, then

the set of orthogonal states thus generated are indistinguishable by one-way LOCC. We then apply these results to distinguish maximally entangled states by one way LOCC.

Maximally entangled states, by definition belong to the family of unilaterally transformable states, although symmetry implies that maximally entangled states are unilaterally transformable in both Alice's and Bob's Hilbert spaces. Maximally entangled states are of considerable importance in quantum information theory and foundations of quantum mechanics because of their role in quantum communication primitives like quantum teleportation and superdense coding as well demonstrating maximal violations of Bell inequalities. Thus local distinguishability of maximally entangled states has attracted a lot of attention in the recent years and one of main open questions in this area is whether a set of $N \leq d$ orthogonal maximally entangled states in $d \otimes d$ can be perfectly distinguished by LOCC for all $d \geq 4$.

To help answer this question we have established an one-to-one correspondence between one-way LOCC distinguishability of a set of orthogonal quantum states and distinguishability of the local unitary operators which generate such a set. With the help of this correspondence we have been able to show that there are sets of $N \leq d$ maximally entangled states in $d \otimes d$ for $d = 4, 5, 6$ such that these states cannot be perfectly distinguished by one way LOCC alone. This provides a strong evidence in support of the conjecture that such sets of states indeed exist. Very recently in [22] a set of four maximally entangled states in $4 \otimes 4$ are presented that are not perfectly distinguishable by PPT operations, and therefore by LOCC but the question in higher dimensions remain open. We conjecture that these examples are potentially strong candidates to establish that any N maximally entangled states in $d \otimes d$ may not be perfectly distinguished by LOCC even if $N \leq d$. We believe that a resonable way to conclusively answer this question would be to extend the applicability of the necessary condition presented in this paper (see Proposition 1 and Corollary 3 for maximally entangled states) to two-way LOCC protocols.

A very interesting avenue of further research based on the results presented here would be to extend these results in multipartite systems. For multipartite systems, unless for very special cases, the extension is not straightforward and generally gives rise to complex scenarios. To illustrate let us consider the simplest multipartite scenario consisting of three parties Alice, Bob and Charlie. Assume that the set of states are being generated by applying unitary operations on some standard state, either on the local Hilbert

space of Bob or Charlie or both. Then a straightforward generalization of the bipartite case now gives rise several independent cases corresponding to the following forms of unitary operations: (a) $\{I \otimes U_i \otimes I\}$, (b) $\{I \otimes I \otimes V_j\}$, and (c) $\{I \otimes U_i \otimes V_j\}$. The interesting cases are when the unitary operators $\{U_i\}$ and $\{V_j\}$ are not perfectly distinguishable on the local Hilbert spaces they act upon, and instead can be perfectly distinguished in an extended tensor product space.

In the first two cases it is possible to obtain results similar to that obtained in this work with respect to the following one way LOCC in the directions $A \to C \to B$ for case (a), and $A \to B \to C$ for case (b). On the other hand case (c) merits careful consideration, and it is not obvious at all how the results in this paper could be generalized to include such cases. Thus for a general multipartite system consisting of say, N subsystems, our results can be applied when the states can be mapped onto one another by applying local unitaries only one one subsystem. For more complex scenarios that involve unitaries mapping the states onto one another by acting on two or more subsystems would call for further research and beyond the scope of this paper.

Finally we would like to mention that quantum cryptography primitives like both classical and quantum data hiding, secret sharing protocols [23–26] make use of the fact that it is not possible to perfectly determine the state of a quantum system even though it was prepared in one of several orthogonal states. In this paper several examples of locally one-way indistinguishable minimal (possibly) sets of maximally entangled states are presented with the property that they are unilaterally transformable. It is conceivable that these states with their very special properties may find applications in developing new protocols for secret sharing and data hiding.

Acknowledgments

SG kindly acknowledges the hospitality of Bose Institute, Kolkata and ISI, Kolkata during his visits in 2010 when part of the work was completed.

[1] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Physical Review A 59, 1070 (1999).

[2] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible product bases and bound entanglement, Physical Review Letters 82, 5385 (1999).

[3] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local distinguishability of multipartite orthogonal quantum states, Physical Review Letters 85, 4972 (2000).

[4] J. Walgate and L. Hardy, Nonlocality, asymmetry and distinguishing bipartite states, Physical Review Letters 89, 147901 (2002).

[5] S. Ghosh, G. Kar, A. Roy, A. Sen (De), and U. Sen, Distinguishability of Bell states, Physical Review Letters 87, 277902 (2001).

[6] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen (De), and U. Sen, Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement Physical Review A 65, 062307 (2002).

[7] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Distinguishability of maximally entangled states, Physical Review A 70, 022304 (2004).

[8] P. -X. Chen and C. -Z. Li, Orthogonality and distinguishability: criterion for local distinguishability of arbitrary orthogonal states, Physical Review A 68, 062107 (2003).

[9] H. Fan, Distinguishability and indistinguishability by local operations and classical communication, Physical Review Letters 92, 177905 (2004).

[10] M. Horodecki, A. Sen (De), U. Sen, and K. Horodecki, Local distinguishability: more nonlocality with less entanglement, Physical Review Letters 90, 047902 (2003).

[11] M. Nathanson, Distinguishing bipartite orthogonal states by LOCC: best and worst cases, Journal of Mathematical Physics 46, 062103 (2005).

[12] J. Watrous, Bipartite subspaces having no bases distinguishable by local operations and classical communication, Physical Review Letters 95, 080505 (2005).

[13] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, Bounds on entangled orthogonal state discrimination using local operations and classical communication, Physical Review Letters 96, 040501 (2006).

[14] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication, Physical Review Letters 98, 230502 (2007).

[15] R. Y. Duan, Y. Feng, Y. Xin, and M. S. Ying, Distinguishability of quantum states by separable operations, IEEE Trans. Inform. Theory 55, 1320 (2009),

[16] S. Bandyopadhyay and J. Walgate, Local distinguishability of any three quantum states, J. Phys. A: Math. Theor. 42 (2009) 072002.

[17] S. Bandyopadhyay, Entanglement and perfect discrimination of a class of multiqubit states by local operations and classical communication, Physical Review A 81, 022327 (2010).

[18] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Optimal local discrimination of two multipartite pure states, Physics Letters A 288, 62 (2001).

[19] Y. -X. Chen, and D. Yang, Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communication, Physical Review A 65, 022320 (2002).

[20] A. Chefles, Condition for unambiguous state discrimination using local operations and classical communication, Physical Review A 69, 050307 (2004).

[21] S. M. Cohen, Local distinguishability with preservation of entanglement, Physical Review A 75, 052313 (2007).

[22] N. Yu, R. Y. Duan, and M. S. Ying, Distinguishing Maximally Entangled States by PPT Operations and Entanglement Catalysis Discrimination, arXiv:1107.3224.

[23] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Hiding bits in Bell states, Physical Review Letters 86, 5807 (2001).

[24] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory 48, 580 (2002).

[25] T. Eggeling, and R. F. Werner, Hiding classical data in multipartite quantum states, Physical Review Letters 89, 097905 (2002).

[26] D. Markham and Barry C. Sanders, Graph states for quantum secret sharing, Physical Review A 78, 042309 (2008).